

REMARKS

The application has been amended and is believed to be in condition for allowance.

Claims 1-13 were examined.

Claims 2, 3, 9, and 11-13 were rejected under §112, second paragraph, as indefinite.

The previously pending claims have been replaced with new claims drafted to take into account the bases of rejection under §112. Withdrawal of the indefiniteness rejection is solicited.

Claims 1-3 and 7-10 were rejected as anticipated by ODINAK 6,690,289.

Claim 4 was rejected as obvious in further view of BRAINARD 6,985,583.

Claims 5 and 6 were rejected as obvious in further view of OSMOND 6,044,468.

Claims 11-13 were rejected as obvious in further view of GRAVEMAN 6,851,052.

The subject matter of the new independent claims now more specifically recites simple network management protocol (SNMP). In particular, the subject matter of the independent claims has been revised to contain the feature that the authentication string is arranged to be incorporated into a communal string field of the simple network management protocol.

As acknowledged in the Official Action ODINAK does not teach the SNMP.

OSMOND teaches SNMP using a specific security transmission system. OSMOND, however, does not teach the recited feature of the present invention. Thus, the combination of ODINAK and OSMOND fails to teach that the communal string field of the simple network management protocol is used for carrying the authentication string for security.

In the claimed invention, an authentication string to be applied once, and based on a shared seed between the client and the agent, is incorporated into a communal string field of a simple network management protocol message to be transmitted between the client and the agent. Further, the claims require that the string be determined by a substantially similar algorithm at both the client and the agent based on the shared seed.

The present invention provides clear benefits by utilizing the communal string field of SNMP messages for incorporating and carrying the authentication string for security purposes. Thus, the present invention can use the structures and protocols of the SNMP. These structures and protocols are existing by the SNMP standard, thereby the present invention is very compatible with this standard.

Reference is made to the Detailed Description of the Embodiments section of the specification. Therein it is

disclosed that the invention's preferred embodiments applies a communal authentication string field of the SNMP message to secure set based operation between the agent and the client. Each communal authentication string is applied only once and each new one is determined with the same algorithm at both ends. The algorithm is based on a shared random seed and can provide the system with required security by complex enough creation of the new communal string from the seed.

In a further embodiment as disclosed, the simple network management protocol message comprises three parts: a protocol version, the communal string field, and a data area divided into protocol data units. The communal string field is a Simple Network Management Protocol community identifier. The Simple Network Management Protocol message applies ASN-1 encoding, and the communal string field is stored in a character string.

Furthermore, in another further embodiment the secure algorithm program can be based on, for example, MD5, MD2, and MD4. MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input that is claimed to be as unique to that specific data as a fingerprint is to the specific individual.

See the embodiments of Figure 4 showing in step 400 the seed being established. The seed is generated by the random

number generator program and the seed is contained in the PDU field of the SNMP message.

Applicant has carefully studied each of ODINAK, BRAINARD, OSMOND, and GRAVEMAN. Applicant does not see that any of these references teaches the claimed features of the invention. Nor does any reasonable combination of these references suggests the claimed features.

None of the references teaches the recited authentication string applied once to a communal string field of a simple network management protocol message, where the authentication string is based on a shared seed between the client and the agent, the first authentication string determined by a substantially similar algorithm at both the client and the agent using the shared seed.

Accordingly, each of the independent claims is believed patentable.


The dependent claims are also believed patentable, at least for depending from an allowable claim.

Reconsideration and allowance of all the claims are respectfully requested.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON



---

Roland E. Long, Jr., Reg. No. 41,949  
745 South 23<sup>rd</sup> Street  
Arlington, VA 22202  
Telephone (703) 521-2297  
Telefax (703) 685-0573  
(703) 979-4709

REL/lrs